

RANDERS

Databeskyttelsesforordningen i praksis
Tandplejen

HVEM OG HVAD

Maria Lotte Tolstrup Christensen
Fungerende databeskyttelsesrådgiver i Randers Kommune og
jurist

Hvorfor en Databeskyttelsesrådgiver?

Lovkrævet funktion jf. Databeskyttelsesforordningen (25. maj 2018)

Hvad skal en Databeskyttelsesrådgiver?

- Rådgive jf. databeskyttelsesforordningen og –loven
- Overvåge overholdelse – intern kontrol
- Kontaktperson for de registrerede
- Kontaktperson til Datatilsynet

Kontakt:

Maria.lotte.christensen@randers.dk / dpo@randers.dk / mobil: 51
56 28 00

HVAD ER EN PERSONOPLYSNING?

Artikel 6

Almindelige personoplysninger

- Navn
- Adresse og kontaktoplysninger
- Fødselsdato
- Oplysninger om beskæftigelse
- Købshistorik
- Visse familiære relationer

Fortrolige personoplysninger

- Ansøgninger og CV'er
- Personlighedstest
- Oplysninger om indtægts- og formueforhold,, herunder SKAT, gæld m.v.
- Oplysninger om sygedage
- Oplysninger om separation og skilsmisse
- Oplysninger om økonomiske forhold
- Oplysninger om rent sociale forhold
- CPR-nummer

Ikke udtømmende – blot eksempler

Artikel 9

Følsomme personoplysninger

- Race eller etnisk oprindelse
- Politisk overbevisning
- Religiøs overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske data
- Biometriske data med det formål entydigt at identificere en fysisk person
- Helbredsoplysninger
- Oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

OBS: Denne liste er udtømmende

Artikel 10

Oplysninger vedr. straffedomme eller lovovertrædelser

- Straffeattest
- Andre sanktioner som f.eks. rettighedsfrakendelse
- Anmeldelser til politiet, som må anses for at være underbygget.
- Oplysning om sigtelser

Ikke udtømmende – blot eksempler

CPR-nummer:

Databeskyttelseslovens §11

Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer

Når du behandler personoplysninger er det vigtigt, at du kender formålet, hvilken type oplysninger der behandles samt hvilket hjemmel som ligger til grund for en lovlig behandlingen.

Kend formål og hjemmel – husk at dokumenterer!



PRINCIPPERNE FOR BEHANDLING AF PERSONOPLYSNINGER

Principperne for behandling af personoplysninger er et godt redskab at arbejde efter, når databeskyttelsesforordningen skal overholdes.

Lovlighed, rimelighed og gennemsigtighed

Dette indebærer bl.a., at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen.

Rigtighed

Oplysningerne skal være rigtige og ajourførte, og hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.

Formålsbegrænsning

Formålet med behandling skal være udtrykkeligt angivet og legitimt. Derudover må eventuel senere behandling ikke være uforenelig med det oprindelige formål.

Opbevaringsbegrænsning

Personoplysningerne må kun opbevares, så længe det er nødvendigt.

Dataminimering:

Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet.

Integritet og fortrolighed

Oplysninger skal beskyttes mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget.

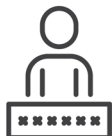
GODE TOMMELFINGERREGLER

IFT. GDPR OG INFORMATIONSSIKKERHED



Låst skærm

Lås altid din PC, når du går fra den - benyt tastaturgenvejen **Win + L**
Husk også at låse smartphones og tablets.



Adgangskode

Lav unikke og gerne lange kodeord - og hold dine adgangskoder for dig selv.



Ryd op på dit skrivebord!

Hav ikke fortrolige og følsomme oplysninger på dit skrivebord – dette gælder også skrivebordet på din PC.

Husk også oprydning på din smartphone og tablet



Print

Benyt Follow you-print når du printer - eller hent dine print med det samme!



Papir

Opbevar papir med fortrolige og følsomme oplysninger, hvor uvedkommende ikke har adgang til dem, fx i aflåste skabe.



Journalisering og arkivering

Journaliser og arkiver dine dokumenter i fagsystem – ikke på dit skrivebord eller på drev.

Husk journaliseringspligten!



Registrering

Registrer kun oplysninger, som er relevante for sagen.



Behandlingshjemmel

Har du hjemmel til behandling af personoplysninger? - Husk at oplysninger må kun behandles til det formål, de er indhentet til.



Mail

Mails indeholdende fortrolige og følsomme personoplysninger, må max ligge 30 dage i Outlook. Journaliser løbende og slet i Outlook.



Kalender

Skriv ikke personoplysninger, som f.eks. CPR-nummer, i emnefeltet på kalenderaftaler i Outlook. Det samme er gældende i emnefeltet i mails, da det ikke krypteres.



Korrekt modtager?

Vær opmærksomhed på, om digital post sendes til rette modtager. Har du mere end en sag åben – så dobbelttjek modtageren og eventuelle bilag inden afsendelse.

- og send altid personoplysninger på en sikker måde, fx via digital post.

OBS: Fordi du må – betyder det ikke at du har hjemmel til udvekslingen.

UDVEKSLING AF OPLYSNINGER

Gælder også når udveksling sker via Outlook

Hvordan må jeg udveksle oplysninger til andre?

Kategori	Intern mail @randers.dk til @randers.dk	Intern mail til ekstern mail @randers.dk til fx @hotmail.com	Sikker mail via "Send sikkert"- funktion i Outlook	Digital post / e-Boks	Via fag- system	SMS	Fysisk post
Følsomme og fortrolige personoplysninger samt CPR-nummer							
Almindelige personoplysning							
Andre oplysninger							

Symbolforklaring:



Del du bare her!



Her må godt deles almindelige personoplysninger, men det er vigtigt, at du er opmærksom på, at almindelige personoplysninger skal behandles som var de følsomme oplysninger, hvis flere af oplysningerne bliver koblet sammen, så oplysningerne samlet bliver personhenførbare. Er du i tvivl? Så gem ikke personoplysninger her.



STOP – personoplysninger må du ikke dele her!!!

HVOR MÅ JEG GEMME PERSONOPLYSNINGER?

Hvor må jeg gemme personoplysninger?

Kategori	Lokalt på PC / tablet / mobil	Ekstern harddisk / USB-stik	Drev	Outlook	SBSYS	Fag- system fx NOVAX	Fysisk
Følsomme og fortrolige personoplysninger samt CPR-nummer							 *Skal være låst inde
Almindelige personoplysning							 *Skal være låst inde
Andre oplysninger							

Symbolforklaring:



Gem du bare
her!



Her må godt gemmes almindelige personoplysninger, men det er vigtigt, at du er opmærksom på, at almindelige personoplysninger skal behandles som var de følsomme oplysninger, hvis flere af oplysningerne bliver koblet sammen, så oplysningerne samlet bliver personhenførbare. Er du i tvivl? Så gem ikke personoplysninger her.



STOP –
personoplysninger må du
ikke gemme her!!!

MÅ JEG SENDE SMS'ER?

SMS-kommunikation bør ikke anvendes til sagsbehandling, da indhold med følsomme eller fortrolige oplysninger skal sendes via en sikker (krypteret) løsning, som f.eks. digital post.

Kommunikation via **SMS kan som udgangspunkt udelukkende bruges til at give påmindelser og kortere servicebeskeder**, eksempelvis:

- ☒ Husk din aftale (dato/kl.) med Randers Kommune, (adresse). Evt. afbud på (tlf.nr/emailadresse).

OBS: SMS-teksten må ikke komme med nogen nærmere angivelse af indgang/adresse, hvis den i sig selv afslører en så specifik afdeling, at der reelt er beskrevet en følsom/fortrolig oplysning – f.eks. indgangen til rusmiddelcentret.

- ☒ Vi har indsat 2.400 kr. på din konto. Mvh. Randers Kommune.

Bruges SMS til påmindelser og kortere servicebeskeder, husk:

Journalisering: Indhold og afsendelse af SMS skal kunne dokumenteres.

Indhent samtykke: Borgeren skal klart have sagt JA til, at der benyttes SMS.

Husk at modtage sms'er også er omfattet af notat- og journaliseringspligten!



UDSATTE BORGERE:

I nogle særlige tilfælde kan SMS'er med følsomt/fortroligt indhold accepteres som kommunikationsform grundet tungtvejende hensyn til borgeren f.eks. hvis dette er eneste måde, at imødekomme en borgers rettigheder efter serviceloven baseret på et socialfagligt eller lægelige skøn. Denne vurdering skal ske individuelt og skal dokumenteres.

Vil du vide mere om brugen af SMS, så se retningslinjen for kommunikation via SMS med borgere på Broen under Jura ⇒ EU's databeskyttelsesforordning ⇒ Interne vejledninger.

BRUD PÅ PERSONDATASIKKERHEDEN

Brud på persondatasikkerheden skal som udgangspunkt anmeldes til Datatilsynet.

En anmeldelse af et brud på persondatasikkerheden, skal om muligt ske inden for 72 timer fra at bruddet er konstateret.

Det er derfor vigtigt, at du indberetter brud til databeskyttelsesrådgiver, så snart du har opdaget den.

Indberet brud via IT support ikonet på dit skrivebord.

Vælg herefter "Anmeld brud på persondatasikkerheden"

